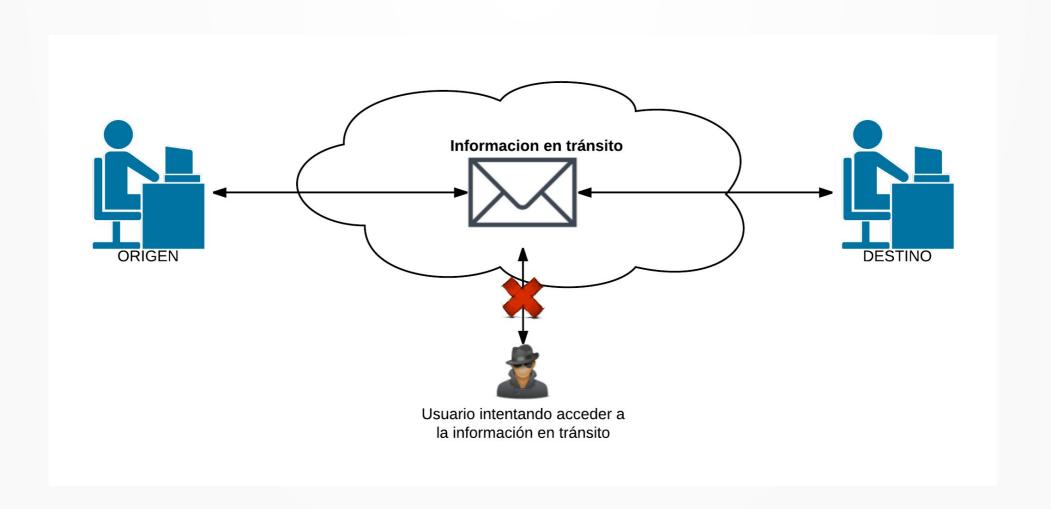
# Seguridad de Redes

- Requerimientos
- Integridad
- Autenticidad
- Sistemas de cifrado

# Objetivo

- Seguridad de redes puede significar muchas cosas, entre ellas:
  - Control de Acceso a la red
  - "Hardening" de equipos en la red
  - Filtrado de trafico -> "firewalls"
  - Deteccion / Prevencion de intrusos
  - Asegurar la información mientras atraviesa la red

# Objetivo (cont.)



# Requerimientos



# Requerimientos (cont.)



# Requerimientos (cont.) CONFIDENCIALIDAD

La información transmitida, aunque sea capturada, no puede ser comprendida

PAXmšt∕-{7m§yðĀ7¢, ?xβ}ÿmšX^îÜžµ©Û™ fĀćÞ«hʵćfÜ8m¶ŶyĀ&j»å"ir‰j,¶+cyZi»¥j¼Ŷ¢µ'uĉð¢']o cœ7·ŠYhþØ\*iáy§[¡ÜjÖZi»¥j¼Ŷ¢µ'uĉð¢']o cœ7·ŠYhþ[~öċþÖ>•œèx«Ü=iÆÊ%%«×-[)iʧfpôqéc¥§]šx7 EkµÖ›y©;µÛ] Zâu¬μðç-; «ÛMwÛ~9þ/iv×Z† YÛ8mfYyĀ ¢ %yÊ&þCSÈl¢eÛz wf«¾)Ú3 — %%¢fÛ;}¹åjjjÛ7^~)Þi š3Ö«ċw ¹ZžEžm³Èi ˈkyý†Ûjŷûkj{%jx ¢ %yÊ&þø Æ®fÞYö›y©j. ¬ρÛ•CäNf§²V{ö;µBí®Úíu⁻ ¥j{a°Ĭ(v×b,k-¹9ËhmëŏÓJoÛ}·û]µÖ;ç+mşÿðÄ(¢ ^r%e;±æ«r(°%eÝÄ™°!Šv!¥Ébz{wÆÝ; ššš·×ÝŠwšŠV§¶-u°àzÝÄnV§'g»Iæ«rÚjÞpá¶ÚbÚÚŽÉZµċ(¢ ^r%e;¾-Äq«£+§ý°¥j{a°ËZ®Ű6åjy©ŀ•«^ý´ïwûk¶»]j{b™§ ²Æ«bxmv\$á°»k-9EhmēŏÓjö82?d]µÖ;c+m§vðÄ(¢ ^r‰;±æ«r(°%cÝÄ™°sŠvYÉbz{wÆÝ; ššš· xÝŠwšZØiÆ−±\*í; ·pÛ•©äYæÒv°Ütöš†·ŶÜ8m¶Ŷv9¶§²Vz ("Wœçoi∢pÜjēhýévj{b™ § ²Æ«µ°àxÝĀnV§°:ÚžÉZµïÚþ×J°«kµÖåj\~þ×mv\$ìzÇZĒmŽtŰz½´×}tÛ;áþ×muˈkyý†ÛiyūÔ (,Wœcoìy\*܆Ê.Cewpæj»&©©rXžžÝ±\$Ú®&äĀuçāæāj\~µ°àxÝĀnV§´p.læ«rÚjÞpáJÚþÚÚžÉZµè(¢^r‰;¼-Āq«£+§ý,š -+i.pû\*©äNŢ\$²V{ö;µBí®Úſu¹n®+gzÉ?µÛ[%c;ž±Ö>xÓh½ó-z½´x}yā āþ×mu kyýÆÛſÿū0 ("Wœ¢oìy\*܆Ê.Cewpæj×ã©©rXžžÝñ§Ú®&ïÃuçâæå° ë µ\*àzÝÃnV§\*p.Iæ«rÚjÞpá¶ÚþÚÚžÉZµè(e ^r‰;¾-Ãq«-£+§ý¹n®+gzĒ-j, pÛ•©āNJ§²V{ö;µBí®Úſt&©{8°³û]µØ\*'ëk-}6.Ф™ «ÛMwÓMxþ/ívxZ†·ÝŪ8m¶Ýyà ¢°%yÊ&þÇšÈi¢eŰz'wf«¼)Ú5—%%ċéſŰ;}°åjjjŰ7^^)Þ \*^Î\* µ\*àzÝÃnV§\*g›Ĭæ×rÚjÞpæ¶ÚþÚÚZĒZµè(¢ ^r%c;¼-Ãq«-£+§u&©{8~0~ew 'ZžDēj{%jx;kû}}bÚt®x'zÊ®xû]µØ...@'ZÊnNrÚz½'x}4Ó\_âbxmu'kyý†Ûtÿu0 (,Wœcoly'Û†Ê.Çewpæj»â©©rXžžÝ±§Ú®&::Ãuçâç²+';u'àzÝĀnV§'g-Iæ«rÚjÞpæfÚþÚÚžÉZµè(¢ ^r%c;¼-Ãq«-£+\$\C-\\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\circ\$\cir £+\$\!\delta\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles\!particles Æ\$\$PŶ∂°ċ-ci.-pÛ•©ĕNĴ\$²V{ö;μβ(\$ÛſuÔœ\$%;γμÛ]%;2±Ö°Ûœ\$†P˙m58|7×ø;μÛ]ippqfÚv0,Š •c(:ûi:!²-«qèÛ9\$\$ø\$ji)—'\$-pìiō-%c©Φ«pÝyø\$yÖœ\$%cii.-pÛ•©äYæÒy\*Û‡öš†-ŶÛ8mʃŶy¶\$²Vz (,Wœçoï φÜjéhýévuš+e{Z®Ü6åjv©i•«/víwûkJ»luć·«(ú)μØ...®ZËnNrÚz½'x)-cβåbxmu kyýņÜivü0 (,Wœcoiy"܆Ê.Cewpæj»å©©rXžžÝű\$Ú®&;;Aucâc^•ûpi-j·pŮ•©sYæÒy\*ܱöš†-ŸÚ8m¶Ŷy9¶ŝ²Vz (,Wœcoi φÜjehýéyué\_«zŎ«œw ¹ZžDēj{%jx;kû]þÚſ®x^\ïivxbI«nÖ¹Ûsh½6z½´x}täāþxmuˈkyýÆÛiÿū0 (,Wœeoly\*܆Ê,Çewpæj»â©©rXžžÝñ\$Ú®&¦Ãuçâç©%-Ç\$zÖ«œw ¹ZžEžm³ÈiˈkyýÆÛiÿūkj{%jx e %yÊ&bø Æ\$JPŸ+C%cŞ\$ZÖ«ëw 'ZZDēj{%jx;kû]þÚf\$x^2Û\$&&Yþxmv#(Ö\*xÄh½ész½´x}zc\_âþxmu'kyýÆÛiÿü0 (,,Wœ¢oìy\*Û†Ê.Ç¢wpæj»&©©rXžžÝñ§Ú&&:Äuçâç~Jæ«%c©mj.;pÛ+©äYæÒy\*Û‡ö\$†-YÛ8mJŸŶyJ§²Vz (.WœoropOichyéyzEni \$-Ö«cw 'ZZDej{%jx;kû]bÛt@x\_j»!5)azw«bxmv\$\$jeYk-'9EhmeoOjoOj;chu\$yoĀ(¢^r%c;±ce\*r(°%cYĀ\*\*\*j\$vY£bz{wÆYj,\$\$\$ \*YŠwYj»!5)azw«µ\*azYĀnV\$'g·Ize\*rÚj PpdJÚpÚÚZĒZμè(¢ ^r‰; ¼-Āq«£+§ýö«ÞžG§z»Z®Ü6ājy©l•«^ý⁻íwûkJ•]~WZ\*û]μØ'jÛ«u¬μôς-¡·«ÛMw×4þ/ív×Z†·ŸÜ8mJŶyĀ ¢°%yÊ&þÇ8Èl¢êŪz'wſ«¾)Úš—%%cfÜ;}¹ājjjÜ7^~)Þ~WZ\*û]μØ'jÛ«u¬μôς-¡·«ÛMw×4þ/ív×Z†·ŸÜ8mJŶyĀ ¢°%yÊ&þÇ8Èl¢êŪz'wſ«¾)Úš—%%cfÜ;}¹ājjjÜ7^~)Þ~WZ\*ûÖ«èw 'ZZEZm'š-Eï kyý†Ûiyûkj{%jx e\*%yÊ&bø·Æ\$¶ÞŶ+āyēfj.pÛ\*CāNJ\$?V{ō;µBſ®ÛítišŶû]µØ...\$ZËnNrÛz½'×}J\$âþ×mu'kyý†Ûiyü0 ("Wœcoly\*Û†Ē.Cewpæj»&©CrXZZݱ§ÚØ&;;Āucâáj{Z®Ű6åjyy'Zj\*!9';c+m\$ŷf-(,WœgoïφŪjčhýćy,V~²)Pµ\*àzÝÃnV§\*:ÚžÉZµïŪþ×¶»kµØ+iÉ%zĬſvxbI«nÖ²Ūshl⁄cóz½′×}lçāþ×mu″kyýÆÛiÿü0 (,Wœgoìy\*܆Ê.Ç¢wpæj»â©©rXžžÝñ§Ú®&;;Äuçâċ+iÉ%zĔZ®Ü6âjyy′žj·!ý;;ç+m§ÿſ©ì•«^,Š \*c(.uaiU7\*Ú?zà\$\$\*ē-j.-pÛ\*CaNJ\$\*V{ö;µBf@ÚfvY%cx;µÛ}%c;ž±Ö\*ÛcœJ†Þ~m5BM5Bø;µÚ]jÞpáJÚV0,Š \*c(.uj-!2-«qèÜ9\$@øşij\-'5-pilio-%cOC«pÝyø\$zY%cxj,-pÛ\*CaYæÒy\*ܱöš†-ŸU8mJÝYJJ\$\*Vz ("Wœ¢oï φÜjéhýéy... ChuĕZ®Ü6åjy©)•«^ý ſwûkf»|Šbþ×mv\$®Ö°×³h½é>z½´×}4×oåþ×mu\*kyý†Ûjÿü0Ā (,Wœçoìy\*܆Ê.C¢wpæj»å©©rXžžÝ±§Ü®&ïĀuçááèi+Z®Ü6åjyy´žj-¹½;ç+m§ÿf©ì•«^,Š•ç(›ûåŪ7°Ü?zC¢⁻j. ·pÛ+©äN§§²V{ö¿µBſ®ÚſvGrív×b,k-l9ËhmēŏÓ|öߟ·û]µÖ;ç+m§ÿðĀ(¢^r‰;±æ«r(°‰ÝĀ™°ìŠvìYÉbz{wÆŸj,335·×ŸŠw¤z×!µ°àzÝĀnV§°g.Iæ«rÚjÞpá¶ÚþÚÚžĔZµè(¢^r‰;¼-Āq«£+§þGrZ®Üбåjy ©ì•«^° (wûkf»]-EPb×mv#(Ö°ÛSœf†P°m58^'eø;µÛ]iPp@fÚv0.Š•c(›ûi·!²·«qèÜ9\$®ø§iì-'\$·pliö«%o©@vpÝvø§z[§zÖ«ëw 'ZžEžm'šÈi`kvýņÛiÿûkif%ix e\*%vÊ&bø-Æ®fPÝûnëZ®Ü6åiv ©i\*«^\*/\* [wûk¶»]\*\* ~obxmv\$izCZEmŽrÚz½ \*}uÓBâbxmu\*kyóĆÛivüô (,Wœcoiy\*܆Ê.Cewpæi\*â©©rXžžÝı§Ú®&::Aucåcší+Z®Úćâjvv\*ž;†%;c+m§yí©i\*«^.\$ \*c(\*ûâŪ7\*Ú?zæk<i.pÛ\*©äN¶5\*V-{ō; μβ(βÚίγε ŠYZ±û)μØ';Û«υ¬μôc-;·«ÛΜwÓM6b/ίγxZ†·ŶÛ8m¶Ŷγà ¢"%νÊ&bCšÈl¢êÛz'wf«¾)Ú\$— %%«ć(Ū;)\*åijiŪ7~~)p™ è"−V;μ'àzŶÃnV\$'e›læ«τŰiÞoá¶ÚbŰÚžÉZμè(¢ ^r%«; ¾-Ãg«£+8bg ŠYZ†Ö«ëw 'ZZDĕj{%ix;kû]pÛí®xfz'®"¢ë?µÛj'Ê'u¬,6₁₽™ «ÛMwxyb/tvxZ†.ŶÜ8m¶Ŷyà ¢'%yÊ&bÇ3Èl¢ĕÛz'wf«¾)Ú5—%%ċéfÜ;}\*äjjjÜ7^~)Þ™ ĕÞ¶,œŠఁ¬µ'āzÝĀnV§'ç›Iæ«rÚjÞpá¶ÚpÚŰžÉZµċ(¢ ^₁%ċ;¾-Ãq«-£+§þg«zÚár\*.ºÖ«ċw¹ZžDċj{%jx;kû]þÚí®xfŠF£û]µØ'°wZĒ^Í¢+\mèōÓ]ō×M?û]µÖ;ç+m§yðÃ(¢^r%;±æ«r(°%«ÝÙ°\Šv\YÉbz{wÆY],333°×YŠw\ŠF¢Ö«ċw¹ZžEžm³Èi°kyýÆÛiyûkj{%jx¢°%yÊ&þø Æ\$PŶû¢'\$hu'āzÝĀnV\$':ÛžĒZuïÚpxJ\*kuÙ¢'i«?μÛ'Êu-μðÚ/zfP'm58^-āø;μÛ]jPpāſÚy0,Š •ς(-û):¹²-«qċÚ9\$®øşij--'\$-piiö«‰©©«pÝyøşzh-...èjĒZ®Ûćājyy'žj-'[ŷ;ç+mşŷf©]•«^,Š •ς(-ûàÛ7°Ú?zæŠĒ^\ ~µ"àzÝĀnV\$":ÚŹÉZµĭÚþ×J»kµÓ.@f§"O(v×bN«±Ö"ÜfœJ†P"m58møäø;µÜjjÞpáJÚÿ0,Š •ç(\ûj:\!'««qèÜ98@øğj;\-'\$:pìiö«%«©©«pÝyø§xĒ«™ ©l'Ö«ëw 'ZZEZm'\$Èi`kyýÆÜjÿûkj{%jx ¢'%yÊ&þø· Æ®JÞŸó.@f§"KZ® ÜĠġţŷŒţ•«^ŷ ſwûkţ•];('eX;μÛ]%e&° ZĒmfe+imċvÓ]œN·û]μŎ;c+mşŷŎĀ(e ^r%e;±æ×r(°%eŶĀ\*\*\*°ŠvYÉbz{wÆŶ; ššš·×ŶŠw©Š è-+Z®ŪĠġţy 'Z;¹;';;c+mşŷſŒţ•«^,Š•c;·ûâŪ7°Ü?zeŠ è-+Z®ŪĠġţy {ōμβ(®Ú(všè±Ç§Šé;μÛ)'Êu¬μÔÚ/zfP¬m5BM48ø;μÛ]jPp¢fÚy0,Š•ς(·ûj·P·«qèŪ98®ø§j)~§·pìio«‰©©«pÝyø§zšè±Ç§Šéj.-pÛ •©äΥæÒy'܇ōš†·ŸŪ8mfŸyfJ§²Vz (, Wœ¢οϊ·pÛjēhýéy';",qéŝ\*kZ®Ü6åjy ©i-«^y´iwûkJ»]±On,/ivxbI-nÖ\*Ûsh½6:z½'x}tBâbxmu`kyýÆÛiÿü0 (,Wœcoìy\*Û†Ê,Cewpæj-à©©rXžZÝñ\$Ú®&;;Ãucâë-è'µ\*àzÝÃnV\$'p.Iæ«rÚjPpá¶ÚþÚÚžÉZµč(¢ ^r/%;).¼-Ãq«£+\$þÆY°j. -pÛ\*©äNJ\$\*V-{δj,μβ(\$ÛίνC!--)šĺćμÛ|%-&°-ZĒnŽrÚz½'×-)ŧÛåbxmu'kyýÆÛiÿū0 (,Wœçoiy\*Û†Ê,Cewpæj»åCCrXžžÝñŞÚΦ&::Āuçáĕ†X:k7½"àzÝÃnV§'g»Iæ«rÚjÞpáJÚþÚÚžÉZμè(¢ ^γ%ε½-¾-Ãq«£+ŞþC!--)šlémj.-pÛ\*CāNJ§²V-{δįμβίθŰίνC ZY-/ivxbl«nÖ²Üsh½ć×z½′×)wÜÏâpxmu″kyýĆŰiyu0 (,Wœ¢οiy"܆Ê.Çewpæj»â©@rXžžÝñŞÚ®&:;Äuçãe"x"-Xj. pÛ\*©äYæÖy"Üżöš†.ŶÚ8m¶Ÿyy¶ş²Vz (,Wœ¢οiyŪjehýéy±ÊŞ,)eŠŐ«ĕw ¹ZZDëj{%jx;kû]bÚf@xlŠj'\8§fû]µØ'`wZË^f¢+imëöÓ]ŏÓž;dì]µŌ;¢+m§ÿðĀ(¢ ^r%e;±æ«r(°%eÝĀ™¹Šv\YÉbz{wÆÝj, \$35° xÝŠw¬Šj'\8§,Ö«ëw ¹ZžEžm³Ēi⁻kyý†Újŷûkj{%jx ¢°%yÊ&bø Æ®¶ÞŶû°\$ %earlau\*32YAnV8:'UzEZuïÚbx9\*kuÛ\*&±£ûluØ'iÛ\*u:-uôc-; «ÛMwÓMth/iv×Z+ŸÜ8mgYyA c\*%yÊ&bC\$ÈleêUz'wf«¾)Ú\$—%%céÜ;}\*äjjjÜ7^~)Þ\*\*èqÊ-j.-pÛ\*©äYæÖy\*ܱöš†-ŸÜ8mgYy9g\$\*Vz (, Wœeoï mlishosozanii mladanasvini ukuklivirzi ulishosozanii olicimasolini olicimasoli olicimasoli

# Requerimientos (cont.)

#### **INTEGRIDAD**

La información transmitida no se modificó en el camino

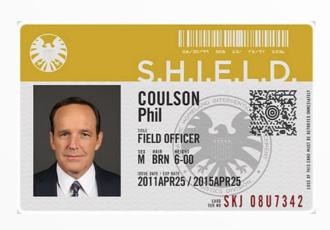




# Requerimientos (cont.)

#### **AUTENTICACION**

La información transmitida proviene de quien dice ser



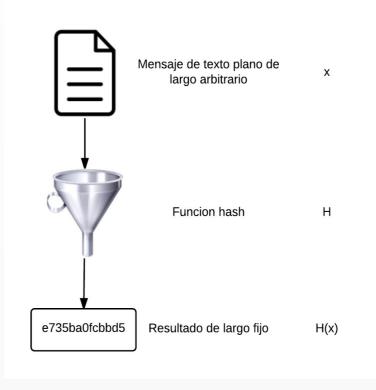


# Integridad

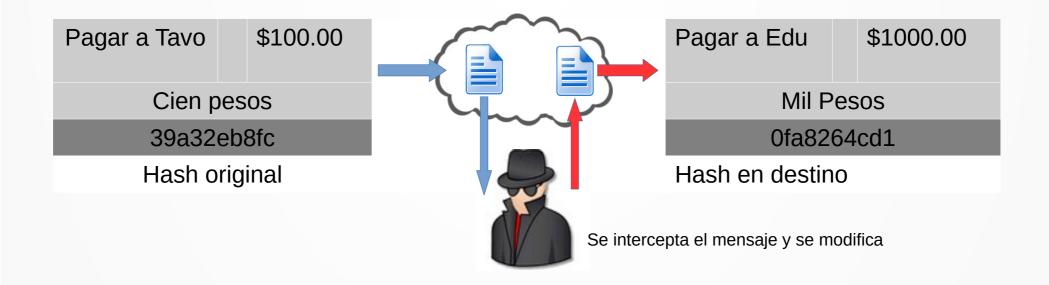
 Para asegurar la integridad se utilizan funciones hash

Funcion matematica en un solo sentido.

Similar al CRC



# Integridad (cont.)



Se debe comparar el hash computado en el destino con el computado en el origen!

# Integridad (cont.)

- Funciones de hash
  - MD5 → valor hash de 128 bits
  - SHA-1 → valor hash de 160 bits
  - SHA-256 → valor hash de 256 bits

http://en.wikipedia.org/wiki/Comparison\_of\_cryptographic\_hash\_functions

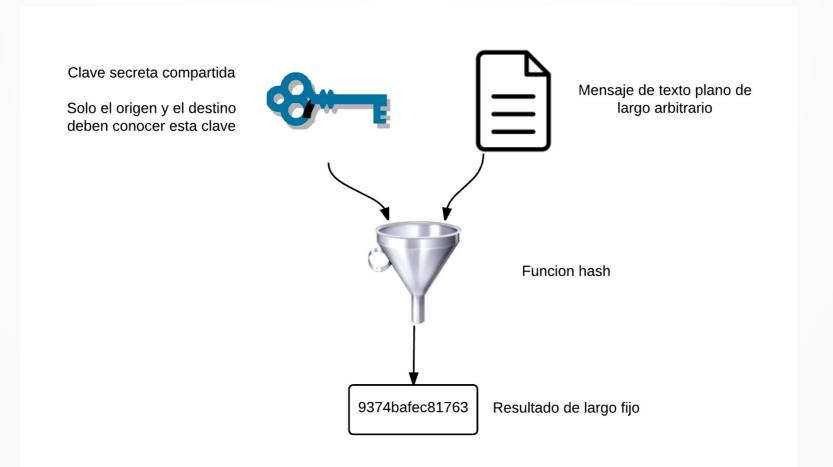
# Integridad (cont.)

- Laboratorio hashes
  - Crear un archivo de texto
  - Obtener el hash de ese archivo
  - Modificar el archivo de texto
  - Obtener el hash del texto modificado y comparar con el valor anterior
  - Comparar con diferentes metodos de hashing
  - Comandos:
    - md5sum
    - sha1sum
    - sha256sum

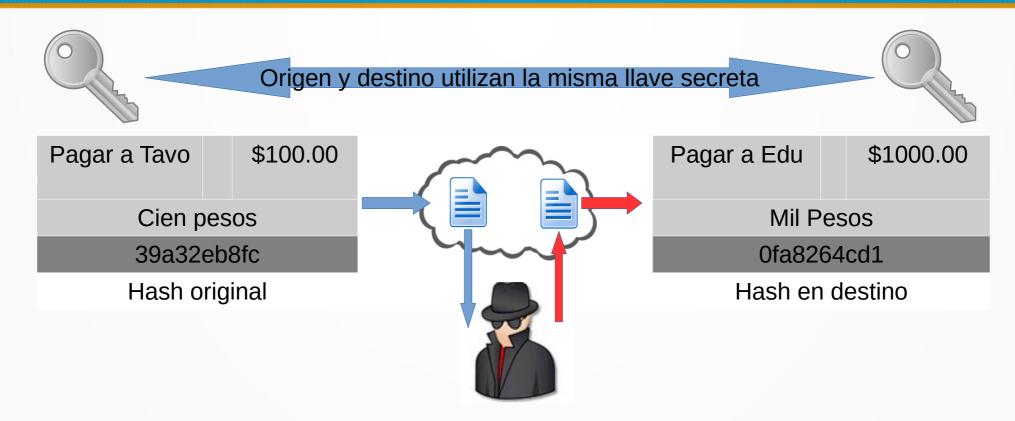
### Integridad + Autenticacion

- Como asegurar que el mensaje no fue alterado (integridad)
- Y proviene de un origen conocido (autenticidad)
- HMAC o KHMAC: Keyed-Hash Message Authentication Code
- Utilizar una llave (clave) compartida agregando autenticidad al hash
- La llave debe ser secreta. Solo debe ser conocida por el origen y el destino

# Integridad + Autenticacion (cont.)



### Integridad + Autenticacion (cont.)



Ya no es completamente necesario comparar el hash de destino con el de origen. Solo se debe computar el hash en el destino utilizando la llave secreta. El valor debe ser completamente diferente si se utilizó una llave falsa.

# Integridad + Autenticacion (cont.)

- Laboratorio HMAC
  - Crear un archivo de texto
  - Crear una clave secreta
  - Generar un HMAC del archivo de texto utilizando la clave secreta
  - Verificar el HMAC si modifica el archivo de texto
  - Verificar el HMAC si modifica la clave secreta
  - Repoducir el procedimiento en diferentes tipos de hash (md5,sha1,sha256)
  - Comandos:
    - openssl dgst -sha1 -hmac "clavesecreta" textoATransmitir.txt

- En un sistema criptográfico es una de las partes mas difíciles de lograr y mantener de manera segura
  - Generación de llave
  - Verificación de llave
  - Transferencia de llave
  - Almacenamiento de llave
  - Duración de la llave
  - Revocar / Eliminar la llave

- Generación de llave
  - Puede ser elegida por el usuario
  - Por lo general es automatizada
  - Se necesita de un buen generador de números al azar
  - Largo/tamaño de llave, en bits.
    - Cuanto mas largo, mejor, pero también consume mayores recursos
  - Keyspace, el numero de posibilidades que se pueden generar con un largo especifico
  - A medida que crece el largo de la llave, el keyspace crece exponencialmente

https://www.keylength.com

- Verificación de llave
  - Casi siempre existen llaves débiles
  - Se deben identificar y regenerar
  - Ej: Cifrado Cesar
    - la llave 0 o la 25 no cifran el mensaje

- Transferencia de llave
  - Se necesita un mecanismo seguro de transferencia
  - Como se ponen de acuerdo ambos extremos de la comunicación
  - Seguramente haciendo uso de un medio inseguro

- Almacenamiento de llave
  - Sistemas operativos modernos son multiusuario
  - La llave puede ser almacenada en memoria para rápido acceso / re-utilización
  - Que pasa si la pagina de memoria debe bajarse a disco?
  - Que mecanismos de protección se utilizan para la información en reposo?

- Duración de la llave
  - Para mejorar la seguridad de los algoritmos de cifrado se debe utilizar una duración acotada
  - Algunos algoritmos utilizan una duración de 24 horas x defecto, ej IPsec
  - Se puede mejorar la seguridad si reducimos el tiempo, por ejemplo a 30 minutos

- Revocar / Eliminar la llave
  - El proceso de revocación debe avisar a todos los interesados que la llave fue comprometida y no debe volver a usarse
  - El proceso de eliminación debe asegurarse que no exista manera de que se pueda recuperar una llave vieja

# Sistemas de cifrado

#### Sistemas de transposición

Alterar el orden de los elementos del mensaje

Е	n		u	n		1	u	9	а
r		d	e		ı	а		M	а
n	С	h	а	,		d	e		С
u	У	0		n	0	m	Ь	r	e
	n	0		q	u	i	e	r	0
	а	С	0	r	d	а	r	m	e

Escítala





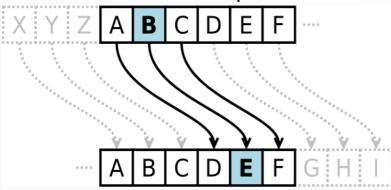
E	r	n	u		
_	1	"	u		
n		С	У	n	а
	d	h	0	0	С
u	e	а			0
n		,	n	q	r
	1		0	u	d
1	а	d	m	i	а
u		e	Ь	e	r
9	M		r	r	m
а	а	С	e	0	e

#### Sistemas de sustitución

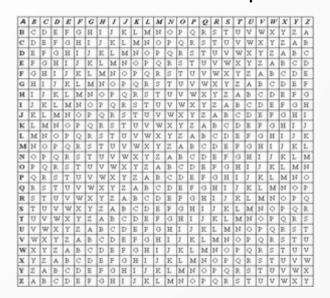
Reemplazar un carácter por otro

Cifrado "cesar" Por desplazamiento, n caracteres Monoalfabético

Palabra clave: n desplazamientos



Cifrado "Vigenère" Polialfabetico Palabra clave se repite





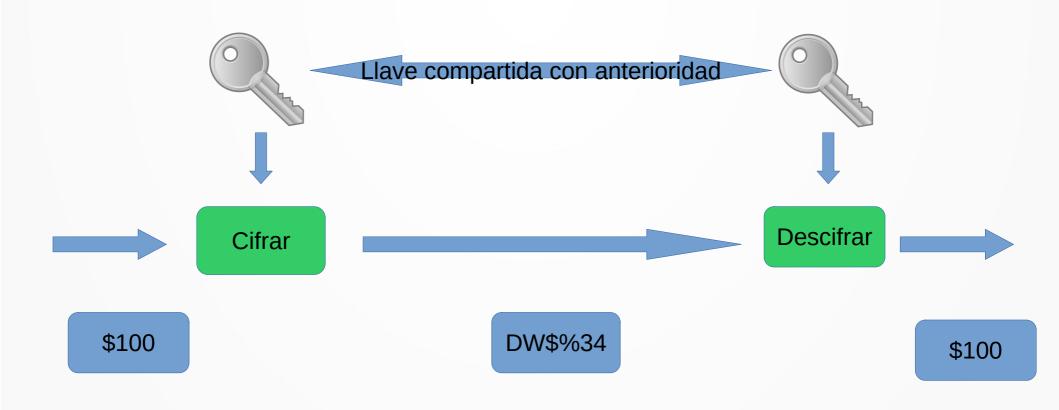
mensaje: PARIS VAUT BIEN UNE MESSEclave: LOUPL OUPL OUPL OUPL OUPL Criptograma: AOMXD KUKE PCTX JHT WSNIO

# Sistemas de "relleno de un solo uso" (one-time pad) Combinación de texto claro con clave aleatoria

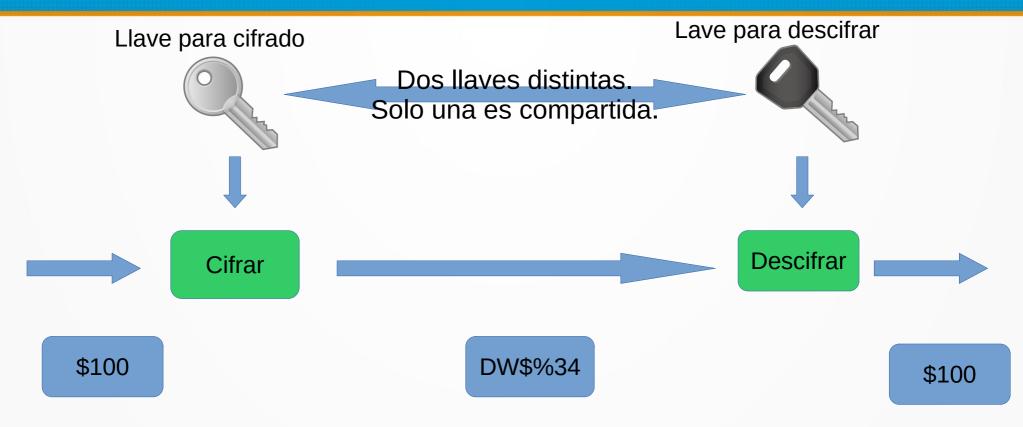
Texto Plano	V	Е	R	Ν	Α	М	С	I	Р	Н	Е	R
Equivalente numerico	21	4	17	13	0	12	2	8	15	7	4	17
+ Numero Aleatorio (CLAVE)	76	48	16	82	44	3	58	11	60	5	48	88
= sum	97	52	33	95	44	15	60	19	75	12	52	105
= mod 26	19	0	7	17	18	15	8	19	28	12	0	1
Texto Cifrado	Т	А	Н	R	S	Р	I	Т	Χ	M	Α	В

- Dos formas de proteger la seguridad de los datos cifrados
  - Proteger el algoritmo
    - Algoritmo secreto. Al ser revelado todos deben cambiar el algoritmo.
  - Proteger la llave
    - En la criptografía moderna todos los algoritmos son públicos

- Dos clases básicas de algoritmos de cifrado protegen las llaves
- Difieren en como utilizan la llave
  - Simétricos
    - Utilizan la "llave secreta" para cifrar y descifrar el mensaje
    - La llave debe ser compartida con anterioridad entre el origen y el destino
  - Asimétricos
    - Utilizan diferentes llaves para cifrar y descifrar el mensaje



Algoritmos de cifrado simétrico Largo de llave típico: 80 a 256 bits Ejemplos: DES, 3DES, AES, Blowfish



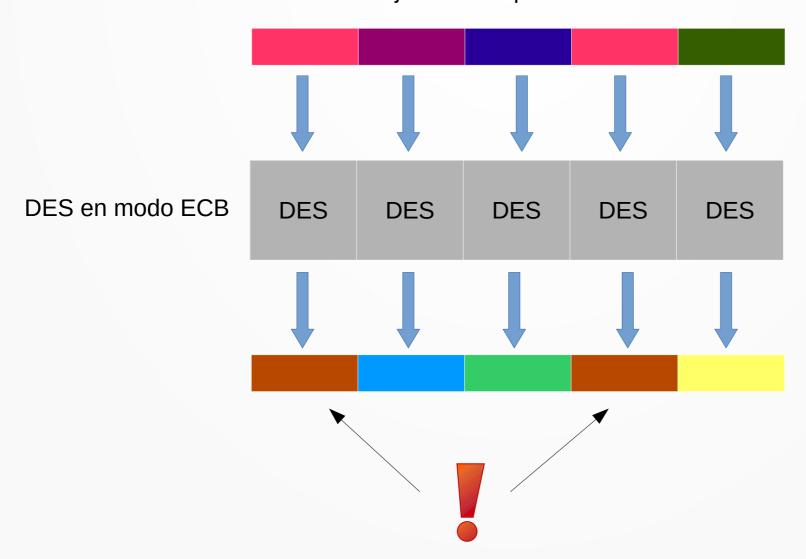
Algoritmos de cifrado Asimétrico Largo de llave típico: 512 a 4096 bits Ejemplos: RSA, ElGamal, DH

### DES

- Data Encryption Standar
  - Algoritmo de cifrado simétrico
  - Generalmente en modo de bloques de 64 bits
    - ECB (Electronic Code Book)
    - CBC (Cipher Block Chaining)
  - Tamaño de llave de 56bits

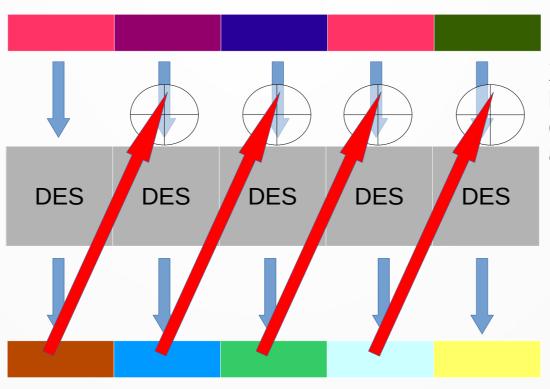
# DES (cont.)

Mensaje de 5 bloques de 64 bits c/u



# DES (cont.)

Mensaje de 5 bloques de 64 bits c/u



XOR bit a bit del bloque de texto con el resultado del bloque anterior

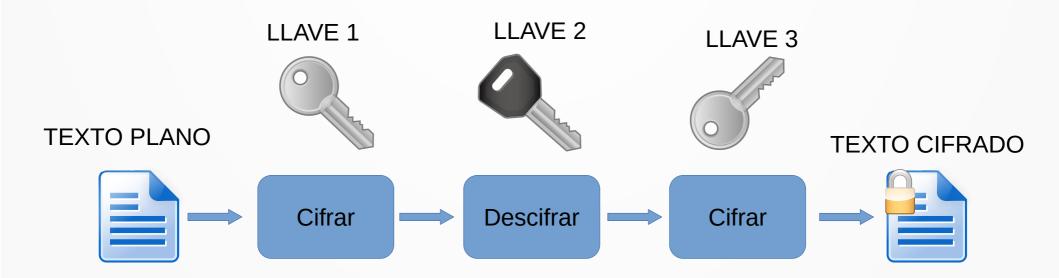
DES en modo CBC

### 3DES

- La llave original de 56 bits resulta muy pobre para los ataques actuales
- En lugar de incrementar la llave (y modificar el algoritmo)
- Usar el mismo algoritmo 3 veces seguidas con diferentes llaves
- Llave de 112 a 168 bits

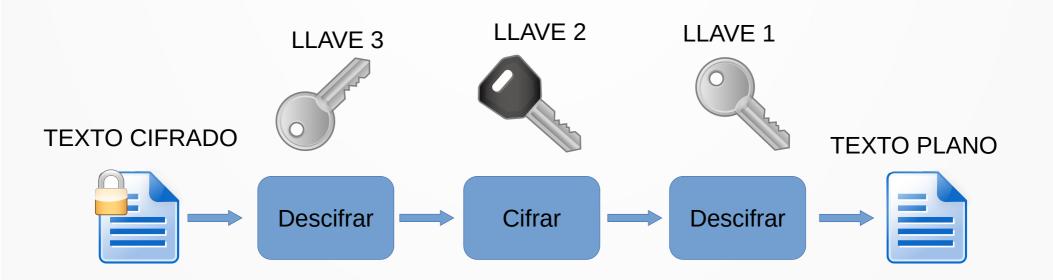
# 3DES (cont.)

#### **CIFRAR**



# 3DES (cont.)

#### **DESCIFRAR**



# Ejercicio

- Realice el ejercicio ECB vs CBC
  - Descargue la imagen Tux.bmp
  - Utilice openssl para cifrar en modos ecb y cbc
  - Verifique los resultados
  - Puede ver la imagen cifrada?

### AES

- Advanced Encryption Standard
  - NIST (National Institute of Standards and Technology) eligió el cifrado Rijndael en 2001 en el que se basa AES
  - Algoritmo de cifrado simétrico
  - Bloques de 128, 192 o 256 bits
  - Llaves de 128, 192 o 256 bits
  - https://formaestudio.com/rijndaelinspector/archi vos/Rijndael\_Animation\_v4\_eng-html5.html

### DH

- Algoritmo Diffie-Hellman
  - Método de intercambio seguro de llaves
  - Se puede utilizar junto con algoritmos simétricos (llave compartida)
  - Permite que el origen y destino generen una llave compartida sin tener un intercambio previo de dicha llave

# DH (cont.)

Alice					
Compartido	Secreto	Calculo			
p=23					
g=5					
	<b>2</b> a = 6				
	3	A = 5^6 mod 23 = 8			

- 1- Alice y Bob se ponen de acuerdo en p (un numero primo) y en g (un numero base, generador)
- 2- Alice y Bob por su cuenta generan un numero secreto (a) y no lo comparten

  $3 - Alice y Bob por su cuenta calculan A = g^a mod p$ 

# DH (cont.)

		Alice	9
	Compartido	Secreto	Calculo
	p=23		
	g=5		
		a = 6	
			$A = 5^6 \mod 23 = 8$
4	A(bob) = 19	5	s = 19^6 mod 23 = 2

4 – Alice y Bob intercambian	el
resultado de A	

5- Alice y Bob por su cuenta calculan  $s = A(del otro)^a \mod p$ 

(s) es la llave secreta

	Bob						
Compartido	Secreto	Calculo					
p=23							
g=5							
	a = 15						
		A = 5^15 mod 23 = 19					
A(alice) = 8	5	s = 8^15 mod 23 = 2					
+	J						

Demo DH en python http://neilrieck.net/dh\_demo.html

### LAB

- Laboratorio AES
  - Crear un archivo de texto
  - Crear una clave secreta
  - Cifrar el texto usando AES con la clave secreta
  - Generar un HMAC del texto cifrado
  - Enviar al destino el texto cifrado y su correpondiente hmac
  - Verificar autenticidad del mensaje cifrado recibido
  - Descifrar mensaje recibido
  - Comandos:
    - openssl enc